End-to-end privacy preserving deep learning on multi-institutional medical imaging

Year: 2021 | Citations: 385 | Authors: Georgios Kaissis, Alexander Ziller, Jonathan Passerat-Palmbach, T. Ryffel, Dmitrii Usynin

Abstract

Using large, multi-national datasets for high-performance medical imaging AI systems requires innovation in privacy-preserving machine learning so models can train on sensitive data without requiring data transfer. Here we present PriMIA (Privacy-preserving Medical Image Analysis), a free, open-source software framework for differentially private, securely aggregated federated learning and encrypted inference on medical imaging data. We test PriMIA using a real-life case study in which an expert-level deep convolutional neural network classifies paediatric chest X-rays; the resulting model's classification performance is on par with locally, non-securely trained models. We theoretically and empirically evaluate our framework's performance and privacy guarantees, and demonstrate that the protections provided prevent the reconstruction of usable data by a gradient-based model inversion attack. Finally, we successfully employ the trained model in an end-to-end encrypted remote inference scenario using secure multi-party computation to prevent the disclosure of the data and the model. Gaining access to medical data to train AI applications can present problems due to patient privacy or proprietary interests. A way forward can be privacy-preserving federated learning schemes. Kaissis, Ziller and colleagues demonstrate here their open source framework for privacy-preserving medical image analysis in a remote inference scenario.